Gordon L. Gibby BEE MS MD
KX4Z
15216 NW 41st Avenue
Newberry FL 32669

April 9 2019

RE: On-The-Air Monitoring of WINLINK Email Demo; Why not done before?

Dear Sirs:

Below I will provide information about a very simple proof-of-concept trial of **on-the-air monitoring of WINLINK communications**, deemed "effectively encrypted" by multiple misinformed commenters. While only a very simple demonstration, it suffices to show that *had anyone been seriously interested in the kinds of monitoring being demanded by proponents of RM-11831, they could have already done so.*

I would then posit that **there is now objective proof that the proponents of RM-11831 were actually NOT seriously interested in their stated goals** (by virtue of their failure to move to complete technically possible solutions). Based on their lack of true, serious belief in the importance of their own stated goal of "on-the-air monitoring," I would ask you to DISMISS RM-11831 and encourage these proponents to carry out the developments that would demonstrate their true interest in their goals, and them come back with a better proposal.

As background, I would explain that many of the proponents of RM-11831 are quite technically accomplished persons, with rather large resources available to them. There include accomplished engineers and professors and persons with significant background in digital signal development, based on their comments on the public forum QRZ.COM. They appear in statements, to have held a concern for national security based on either SCS pactor modems and/or WINLINK for some years. For a concrete example, Professor Rappaport, who indicates he is a world authority in electrical engineering, met with the FCC on September 23, 2016 as as part of his communications to them, he noted

> *"I pointed out national security concerns with the current problem of encrypted data, which arises from the non published compression algorithms used in Pactor II, Pactor III, and Pactor IV, and also discussed how the identification of many ACDS stations are often encrypted, as well, since that is an option on the SCS modems. "*
>
> https://ecfsapi.fcc.gov/file/1110241203910/Reply to Comments NPRM.docx

The Petitioner also states that the lack of the ability to read traffic is a concern of his for dealing with emergencies

> *Furthermore, an amateur radio operator, involved in disaster relief and recovery,*

could be sending legitimate emergency traffic, but without a means to decode it, another station on frequency might continue transmitting, causing interference to the emergency communications, a violation of Part 97.101(c).

Thus whether for emergency operations or national security, proponents of RM-11831, presuming they truly believe their arguments, would have had significant motivation to provide ways to have on-the-air monitoring of WINLINK transmissions, among others. And those concerns, for at least some of them are several years old. Yet they never developed these systems.

Why?

Difficulty? It should not be that difficult for people of these great brilliance and resources. For WINLINK, there is simply NO encryption, despite occasional claims to the contrary. The WINLINK system even disables internal compression within the PACTOR modem, and does not use any encryption of any sort. WINLINK uses publicly documented compression techniques to speed transfer and result precious bandwidth-time utilized. While the compression extends across multiple components of one email and its attachments, expert testimony indicates that it does not extend across emails. (Personal communication, John Wiseman, email personal communication of April 8 2019)

For many years, John Wiseman G8BPQ has provided free software that can handle WINLINK transmissions. His source code is freely available, and in a current programming language. (See: https://github.com/g8bpq/LinBPQ) Many amateur stations utilize his software, even on simple Raspberry Pi $35 micro computers. A map showing scores of stations utilizing his software can be seen at http://nodemap.g8bpq.net:81/

Public discussion has suggested that it would be a modest engineering exercise to take the publicly available compression / decompression provided freely, and apply it to the output of a PACTOR (or any other WINLINK) protocol and as a result turn the messages into instantaneously viewable text. This works much more easily if all the packets are available without corruption, of course and would be more difficult if some packets were missing or corrupted.

However, the proponents of RM-11831 allege that there is a vast majority of people with similar concerns and thus a network of connected diversity receivers (or even web software defined radios) could easily provide a perfect stream of packets from WINLINK systems for the majority of exchanges. (See, https://en.wikipedia.org/wiki/Antenna_diversity and https://en.wikipedia.org/wiki/Diversity_scheme)

Yet this was never developed by the person who state such great concern!

Why?

The WINLINK DEVELOPMENT TEAM has now released a web page that allows any person to view, immediately after transferred, the complete and perfect text of all messages moving through their central message server system (at least for systems not requiring government protection) – not even a

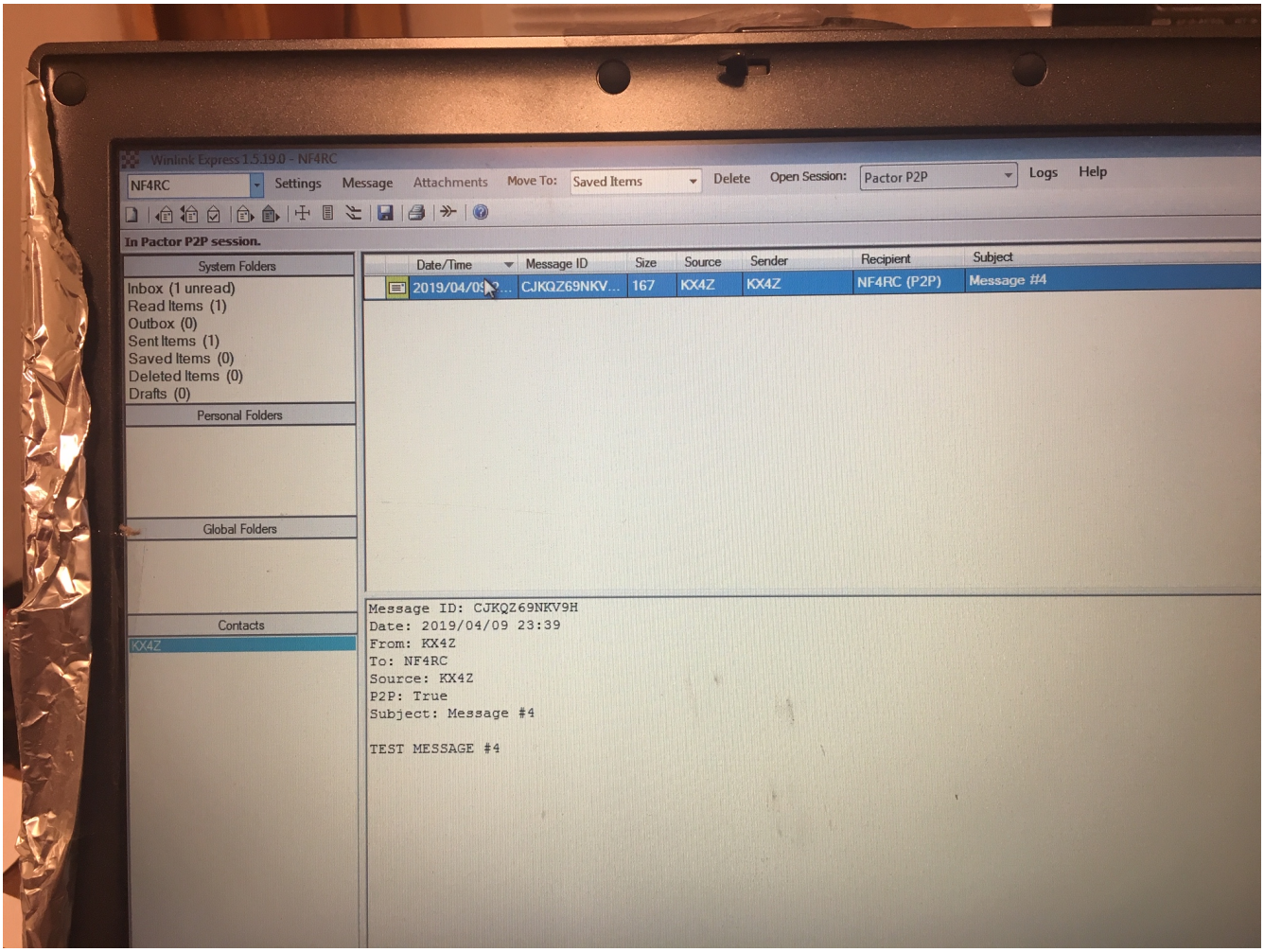
receiver required! (See: https://winlink.org/content/amateur_radio_message_viewer) Proponents of concerns about national security should now be able to monitor every message transferred over the WINLINK central system.

I have already demonstrated that the 97.221(c) "interference' concerns of the Petitioner are mathematically bogus based on an analysis of actual time-bandwidth consumed in a 2-week period on 40 and 20 meters, rendering that portion of the Petitioner's request unsupportable. (See: https://ecfsapi.fcc.gov/file/10408063816674/FCCRM11831-2.pdf)

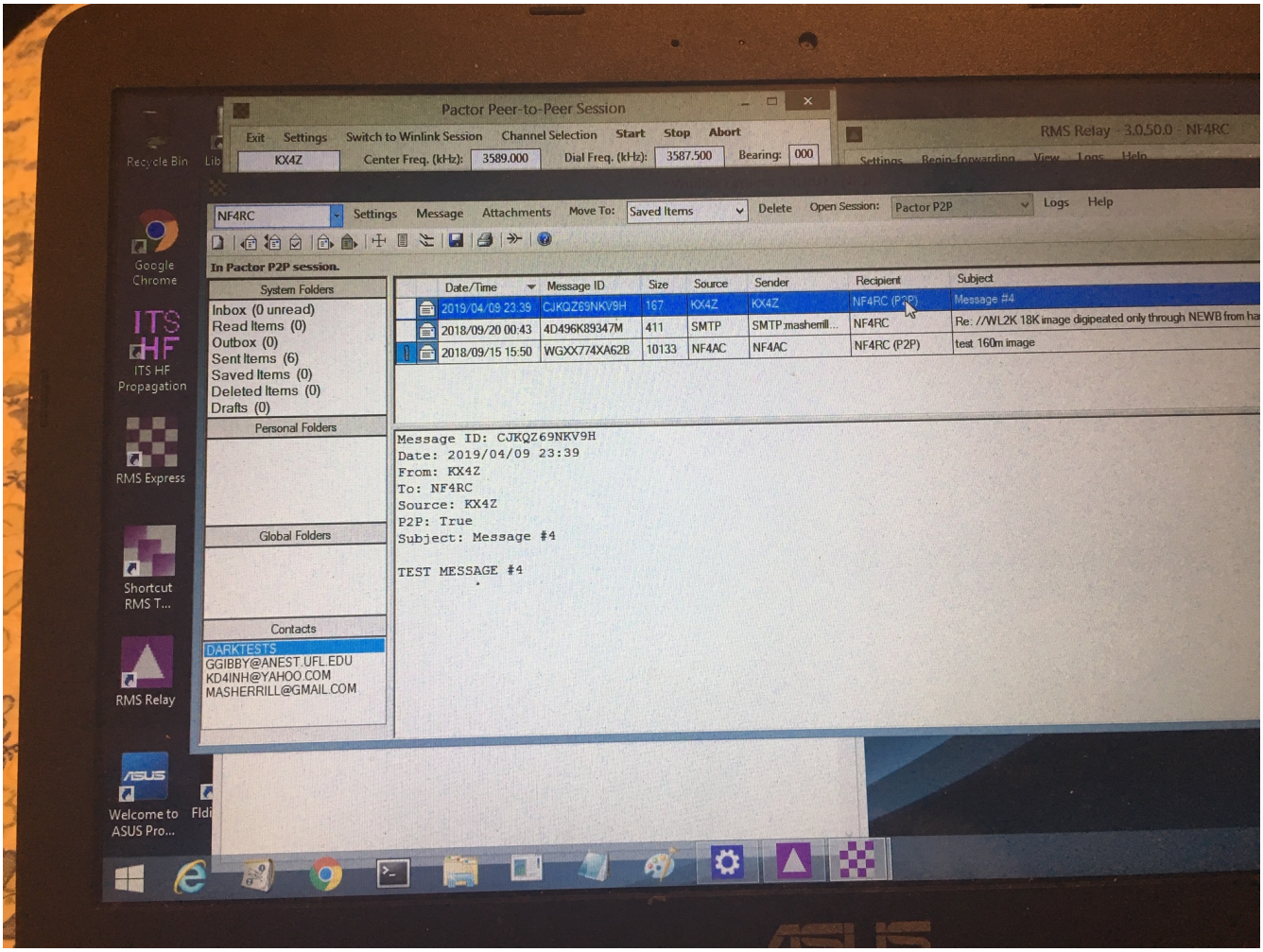
I then pursued discovery of what might be the roadblocks to real creation of an on-the-air monitoring system, so desperately demanded by the proponents of RM-11831.

A very simple proof of concept experiment was carried out. To prove the concept that using free available or simple software to decode WINLINK messages without actually participating in the back-and forth packet acknowledgments requires, for the easiest case, a stream uncorrupted packets. To create that situation, I utilized two amateur radio stations, using two different call signs, in peer-to-peer PACTOR communications on a legal frequency using minimal power and outside antennas on the same property. I then took freely available WINLINK EXPRESS software on another complete WINLINK computer/radio/pactor modem system, and instructed it to attempt to monitor a peer-to-peer message passage as if it were the intended recipient – but it was refused transmit capability by having connection only to a shielded Heathkit dummy load and minimal power, rendering its signal capture and transmission 60 dB below the incredible signals the other two stations were experiencing. The radios involved were simple used ICOM 718's and an older 725. Lacking any ability to make any changes to the software (since I was not using the freely available BPQ code in this experiment) I set transmit delay times to longer than normal so that I could have a reasonable chance of capturing the full packet stream as a diversity receiver system would. The two intended participants easily established communications with the screen indicating very high speed transfer. The third (monitor) station however was able to capture a workable signal and went about its business, fooled into thinking it was part of the conversation using the freely available WINLINK EXPRESS software. Hilariously, the largest problem I faced was running between two receiving stations to answer a dialog box asking whether I wished to accept the proffered message – I enabled the secret monitor station and the intended recipient and the message sped past at blinding speed. This entire experiment took about 30 minutes to set up and complete at my home.

I was rewarded by having **both the participating, intended recipient station AND the secret monitor station capture exactly the same message ("#4 in my subject line") as shown in the photos below** and confirmed by their winlink software lengthy assigned message numbers



Intended receiver station captured messages This ancient VISTA computer is normally utilized for SHARES digital gateway but was re-purposed for this trial.



Monitor Station, Windows 8.1 computer. Exact same message simultaneously captured intact.

Obviously this is only a proof of concept test – but it was done completely over amateur radio frequencies, in real-time, over the air, without any use of the internet at all. I created a situation where perfect packet capture would occur and showed that not even any software development was needed to carry out a simple proof of concept test. **Obviously a skilled person of the stature of some of the advocates of RM-11831 using freely available code from multiple possible sources would be able to do far better than my simple proof of concept test** – and the real question therefore, whether the proponents of RM-11831 actually believe their own claims of the importance of on-the-air monitoring….is answered.

They do *not* believe in their own claims of the importance of on-the-air real-time monitoring.

I am unaware of any such tests carried out, nor any software development carried out, despite their great and self-professed technical talent and their great concern over these matters.

And if the proponents of RM-11831 do not believe in the importance of on-the-air decoding of WINLINK traffic (by far the largest user of PACTOR or other ARQ protocols), then obviously their proposal should obviously be dismissed by the FCC.

Having read the far more reasonable proposal by the Amateur Radio Safety Foundation, published April 9, 2019, I concur completely in their requests. (See: https://ecfsapi.fcc.gov/file/10410668215598/RM-11831%20Motion%20to%20Dismiss%2BPetition.pdf)

Sincerely,

Gordon L. Gibby BEE MS MD
KX4Z